

วารสารสำนักงานคณะกรรมการวิจัยแห่งชาติ

Journal of the National Research Council

EISENSTEIN'S THEOREM AND ARITHMETIC PROPERTIES OF POWER SERIES*

ทฤษฎีบทของไอเซนสไตน์และคุณสมบัติเชิงเลขคณิต
ของอนุกรมกำลัง

Vichian Laohakosol

วิเชียร เล่าหโกศล

Department of Mathematics, Kasetsart University

ภาควิชาคณิตศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

ABSTRACT

We give a short expository account of the classical theorem of Eisenstein, and present some recent results about power series satisfying the Eisenstein condition. These results show that:

- 1. the coefficients of such power series enjoy certain asymptotic properties,*
- 2. such power series assume transcendental or rational values at rational points.*

*The research supported by the Third World Academy of Sciences Research Grant No. 87-47

บทคัดย่อ

งานวิจัยนี้เป็นการศึกษาที่เกี่ยวข้องกับทฤษฎีบทของไอเซนสไตน์ ตลอดจนการแสดงผลใหม่ที่ได้รับเกี่ยวกับอนุกรมกำลังที่คล้ายตามเงื่อนไขของไอเซนสไตน์ ผลที่ได้รับแสดงว่า

1. สัมประสิทธิ์ของอนุกรมกำลังประเภทนี้มีคุณสมบัติเชิงเส้นกำกับบางอย่าง
2. อนุกรมกำลังประเภทนี้มีค่าเป็นจำนวนอดิศัยหรือตรรกยะ ณ จุดตรรกยะ

INTRODUCTION

Well known are the facts that functions analytic about the origin have unique Maclaurin series expansions, and that the coefficients of a power series contain a wealth of information on the function they represent. It is then of interest both analytically and number theoretically to investigate various arithmetical properties of power series in relation to its coefficients. One of the earliest and best known results is the classical theorem of Eisenstein. In this paper, we first give in the next section a brief expository account of this theorem, some of its applications and extensions.

Eisenstein's theorem and its generalizations provide us with a reasonably satisfactory information on the denominators in the coefficients of power series belonging to a large class (the class of Eisensteinian series) containing most algebraic series. One next natural question is to ask for information on the numerators in the coefficients of these series. As mentioned in Popken¹⁷, relatively few results along this line are known. We derive results of this kind for certain power series generalizing those in Popken¹⁷. This is an addendum to our earlier investigation in Laohakosol⁹. Finally, we make a discussion on some open problems.

MATERIALS AND METHODS

In 1852, Eisenstein¹ stated the following theorem, which has been known as Eisenstein's theorem ever since.

The classical Eisenstein's theorem.

$$\text{Let } f(z) = \sum_{n=0}^{\infty} a_n z^n$$

be a power series with rational coefficients. If f is algebraic, i.e. if it satisfies an algebraic equation of the form

$$\sum_{k=0}^K P_k(z) f^k(z) = 0, \quad P_k(z) \not\equiv 0, \quad \dots\dots\dots(1)$$

where K is a positive integer and all $P_k(z)$ are polynomials with rational coefficients, then f satisfies the **Eisenstein condition**, i.e. there exists a positive integer I such that $I^n a_n$ is integral for all $n \geq 1$.

At that time, Eisenstein merely stated this result without supplying a proof. Two years later (1854), Heine³ gave its first proof as well as remarked that we need not have to assume all polynomial coefficients $P_k(z)$ to have rational coefficients.

It is not hard to see that the Eisenstein condition is equivalent to the following pair of conditions:

1. the denominators of the rational coefficients a_1, a_2, \dots contain only finitely many distinct prime factors,
2. $\frac{\log(\text{denominator of } a_n)}{n}$ is bounded for $n = 1, 2, \dots\dots\dots$

Eisenstein's theorem has been found useful in many contexts, principally in verifying that certain functions are transcendental. For example, granted Eisenstein's theorem we can give a very short proof that many well known series such as

1. the exponential series

$$e^z = \sum_{n=0}^{\infty} z^n/n!,$$

2. the logarithmic series

$$\log(1+z) = \sum_{n=1}^{\infty} (-1)^{n+1} z^n/n,$$

- and
3. a Bessel series

$$J_0(\sqrt{-z}) = \sum_{n=0}^{\infty} z^n/n!^2$$

are all transcendental. To see this, we merely observe that the three series contain infinitely many distinct prime factors in the denominators of their rational coefficients and thus cannot be algebraic by Eisenstein's theorem.

Another interesting application is due to Landau⁸, who used it to determine when the hypergeometric series, with rational coefficients, are algebraic. A more recent use of Eisenstein's theorem can be found in Mahler¹¹, who applied it to show that Stäckel's construction of functions¹⁸ which together with their inverses take algebraic values at algebraic points in a neighborhood of the origin does indeed yield transcendental functions.

The converse of Eisenstein's theorem does not hold in general as the following examples show.

1. The series $\sum_{n=0}^{\infty} z^{n!}$ satisfies the Eisenstein condition but it is not algebraic since it has the unit circle as its natural boundary.

2. The series $\sum_{n=0}^{\infty} z^{2^n}/2^{2^n}$ satisfies the Eisenstein condition but its value at $z=1$, say, is transcendental, so it cannot be algebraic for algebraic functions take algebraic values at algebraic points in its domain.

Quite a number of generalizations of Eisenstein's theorem have been obtained so far. We mention here a few of them.

From Eisenstein's theorem, if a_n denotes the n^{th} rational coefficient of an algebraic series, then either $a_n = 0$, or

$$|a_n| \geq e^{-cn} ,$$

for some positive constant c . This corollary of Eisenstein's theorem was extended to power series satisfying linear and algebraic differential equations, where we get for the linear case the lower bound $e^{-c \log n}$, and $e^{-c \log^2 n}$ for the latter case. Further details can be found in Pólya¹³, Popken¹⁵, and Mahler¹¹. Moreover, if p_n denotes the greatest prime factor in the denominator of the rational coefficient a_n (written in reduced fraction), then Eisenstein's theorem implies

$$|P_n| \leq c_1 ,$$

for all n and some positive constant c_1 . This result was extended to power series satisfying linear differential equations by Pincherle¹², and for algebraic differential equations by Hurwitz⁴, where the upper bound reads $c_2 n^{c_3}$, for some positive constants c_2, c_3 . For more details see Popken¹⁶, Kakeya⁵ and Mahler¹¹.

In another direction, Koenigsberger⁷ discussed the coefficients of algebraic power series expanded about an arbitrary point, which reduces to Eisenstein's theorem when the point is the origin.

A more direct generalization, see Pólya and Szegő¹⁴, asserts that Eisenstein's theorem continues to hold if all coefficients $P_k(z)$ are power series with rational coefficients satisfying the Eisenstein condition. In conjunction with this generalization, we are led to the following definition.

Definition. A formal power series $f(z) = \sum_{n=0}^{\infty} a_n z^n$ with algebraic coefficients is said to be **Eisensteinian** if there exists a positive integer I such that $I^n a_n$ is an algebraic integer for all $n \geq 1$.

We gave the following generalization of Eisenstein's theorem⁶.

Theorem. Let $f(z)$ be a power series with algebraic coefficients. If f satisfies an algebraic equation of the form (1) where all $P_k(z)$ are Eisensteinian power series, then f is itself Eisensteinian.

In conclusion of this section, let us mention that a convenient source of information regarding Eisenstein's theorem is in Chapter 3 of Pólya and Szegő¹⁴.

RESULTS

For the rest of this paper, we confine ourselves to Eisensteinian series with rational coefficients. Our aim is to prove certain arithmetic properties about the numerators in the coefficients of these series, and use them to obtain results related to transcendental values taken by such series at rational points. This has been implicitly remarked upon in Laohakosol⁹, and we make it explicit here by giving full details.

Theorem 1. Let $f(z) = \sum_{h=0}^{\infty} a_h z^h$ be an Eisensteinian series with rational coefficients, which is not a polynomial, and convergent in $|z| < R$, where R is a fixed positive number. Let b be a rational number such that $0 < |b| < R$. Put $S_n = \sum_{h=0}^n a_h b^h$ ($n = 0, 1, 2, \dots$) and denote by p_n the largest prime factor in the numerator of S_n (written in reduced fraction).

(1) If $f(b)$ is a nonzero algebraic number, then $\lim_{n \rightarrow \infty} \sup p_n = \infty$.

(2) If $f(b)$ is an irrational algebraic number, then $\lim_{n \rightarrow \infty} p_n = \infty$.

Proof. (1) Since f is Eisensteinian, let I be a positive integer such that $I^h a_h$ is integral for all $h \geq 1$, and let I_0 be the denominator of a_0 . Let $b = u/v$, where u and v (> 0) are rational integers. Then

$$S_n = \sum_{h=0}^n a_h u^h / v^h = x_n / y_n$$

where $y_n = I_0(Iv)^n$, and x_n are rational integers for all n . Denote all prime factors of v by q_1, \dots, q_g . Now assume that the assertion $\lim_{n \rightarrow \infty} \sup p_n = \infty$ is false. Then all integers x_i, y_i have a finite number of prime factors, say q_1, \dots, q_w ($w \geq g$). Thus

$$x_i = \pm q_1^{\xi_1} q_2^{\xi_2} \dots q_w^{\xi_w}, \quad y_i = q_1^{\eta_1} q_2^{\eta_2} \dots q_w^{\eta_w} \quad (i=0, 1, \dots)$$

where the ξ 's and η 's are nonnegative integers. Since $0 < |b| < R$, then there exists a positive number δ so small that

$$\omega := (\delta + 1/R) |b| < 1.$$

Let R ($\geq R$) be the radius of convergence of f . Since $\lim_{h \rightarrow \infty} \sup |a_h|^{1/h} = 1/R'$, then for sufficiently large i , we have

$$\begin{aligned} |f(b) - x_i/y_i| &= \left| \sum_{h=i+1}^{\infty} a_h b^h \right| \leq \sum_{h=i+1}^{\infty} (\delta + 1/R)^h |b|^h \\ &= \omega^{1+i}/(1-\omega). \end{aligned}$$

Choose a positive number ϵ so small that $(I_0 I v)^{-\epsilon} > \omega$. Then for sufficiently large i , we get

$$y_i^{-\epsilon} = (I_0(Iv)^i)^{-\epsilon} > (I_0 I v)^{-i\epsilon} > \omega^i / (1-\omega).$$

Hence, for sufficiently large i ,

$$|f(b) - x_i/y_i| < \omega^i / (1-\omega) < y_i^{-\epsilon}$$

Since $f(b) \neq 0$ is an algebraic number, then by Ridout's theorem¹⁷, we must have

$$f(b) = x_i / y_i \quad \text{for all sufficiently large } i.$$

It follows that $a_i b^i = S_i - S_{i-1} = 0$, and so $a_i = 0$ for all sufficiently large i , which is a contradiction.

(2) The proof is the same as that in part (1). Assuming the assertion is false, then there is an increasing sequence of positive integers (n_j) such that all numerators of S_{n_j} can be formed from a finite number of primes. By the same arguments as before, with (n) now being replaced by (n_j) and S_n by S_{n_j} , we see that for sufficiently large j , $f(b) = x_{n_j} / y_{n_j}$ which contradicts the rationality of $f(b)$.

Theorem 2. Let $f(z) = \sum_{h=0}^{\infty} a_h z^h$ be an Eisensteinian series with rational coefficients.

Suppose f has a pole of first order as its only singularity on the circle of convergence. Let this pole $z=b$ be a rational number. Assume also that f is not of the form polynomial/($z-b$). If p_n denotes the largest prime factor in the numerator of a_n , and if the residue of f at $z=b$ is an algebraic number, then

$$\lim_{n \rightarrow \infty} \sup p_n = \infty.$$

Moreover, if the residue of f at $z=b$ is an algebraic irrational number, then

$$\lim_{n \rightarrow \infty} p_n = \infty.$$

Proof. Consider the function

$$F(z) := (1 - z/b)f(z)$$

which is analytic for $|z| \leq |b|$, so it has the expansion $F(z) = \sum_{n=0}^{\infty} \alpha_n z^n$, which is

Eisensteinian. Let ρ denote the residue of f at $z=b$. Then $F(b) = -\rho/b$. Now applying

Theorem 1(1) with $F(z)$ in place of $f(z)$, we see that the limit superior of the greatest prime

factors in the numerators of $\sum_{h=0}^{n_i} \alpha_h b^h$ is infinite. On the other hand, $\sum_{h=0}^{n_i} \alpha_h b^h$ is

the coefficient of z^{n_i} in the Taylor expansion of

$$\frac{F(bz)}{1 - z} = f(bz).$$

Hence,

$$\sum_{h=0}^{n_i} \alpha_h b^h = a_{n_i} b^{n_i}$$

and the first assertion follows.

To prove the second assertion, we proceed as above by replacing n_i by n , applying Theorem 1(2) and noting that $F(b) = -\rho/b$ is algebraic irrational.

Theorem 3. Let $f(z) = \sum_{h=0}^{\infty} a_h z^h$ be an Eisensteinian series with rational coefficients, having a positive radius of convergence R , and let α be a nonzero algebraic number satisfying $|\alpha| < R$. Assume that there are two sequences of nonnegative integers (r_n) and (s_n) such that

$$0 = s_0 \leq r_1 < s_1 \leq r_2 < s_2 \leq r_3 < s_3 \leq \dots, \quad \lim_{n \rightarrow \infty} s_n / r_n = \infty,$$

and

$$a_h = 0 \text{ if } r_n < h < s_n, \text{ but } a_{r_n} \neq 0, a_{s_n} \neq 0 \text{ (} n=1, 2, 3, \dots \text{),}$$

$$a_0 \text{ may or may not be } 0.$$

Put

$$Q_n(z) = \sum_{h=s_n}^{r_{n+1}} a_h z^h$$

Then $f(\alpha)$ is algebraic if and only if there exists a positive integer $N = N(\alpha)$ such that $Q_n(\alpha) = 0$ for all $n \geq N$.

Proof. The sufficiency of the condition is obvious. We proceed to show that it is also necessary. Assume

$$f(\alpha) = \sum_{h=0}^{\infty} a_h \alpha^h = \beta$$

is an algebraic number of degree t over the rationals. Let

$$\beta^{(0)} = \beta, \beta^{(1)}, \dots, \beta^{(t-1)}$$

be all its conjugates and let c_0 be a positive integer such that $c_0\beta, c_0\beta^{(1)}, \dots, c_0\beta^{(t-1)}$ are all algebraic integers.

In what follows c_1, c_2, \dots denote positive constants that may depend on $\alpha, \beta, \beta^{(1)}, \dots, \beta^{(t-1)}$ but are independent of n . Choose c_1 so that

$$|\alpha| < 1/c_1 < R, \text{ so } |c_1\alpha| < 1$$

and c_2 so that

$$|a_h| \leq c_1^h c_2 \quad \text{for all } h \geq 0.$$

Put

$$P_{n\sigma}(z) = -\beta^{(\sigma)} + \sum_{h=0}^{r_n} a_h z^h \quad (n=0, 1, \dots).$$

Since f is Eisensteinian, let I be a positive integer such that Ia_0 and $I^h a_h$ are integral for all positive integer h . Also put

$$P_n(z) = c_0^t I^{r_n t} \prod_{\sigma=0}^{t-1} P_{n\sigma}(z).$$

Clearly, $p_n(z)$ is a polynomial in z of degree $r_n t$ with integral coefficients. By a length inequality,¹⁰

$$L(p_{n\sigma}) \leq |\beta^{(\sigma)}| + \sum_{h=0}^{r_n} |a_h| \leq c_1^{r_n} c_3,$$

where $L(P)$ is the sum of absolute values of each coefficient of the polynomial P , the so-called length of P . Here and throughout this proof, we tacitly assume $c_1 \geq 1$. If $c_1 < 1$, the main arguments hold with only slight modification. Therefore,

$$L(p_n) \leq c_0^t I^{r_n t} (c_1^{r_n} c_3)^t \leq (c_1 I)^{t r_n} c_4.$$

Thus for all $n \geq N_0$,

$$Q_n(\alpha) = \sum_{h=0}^{r_{n+1}} a_h \alpha^h - \sum_{h=0}^{r_n} a_h \alpha^h = \beta^{(\sigma_{n+1})} - \beta^{(\sigma_n)}.$$

Since the series for $f(\alpha)$ converges, then $P_n(\alpha) \rightarrow 0$ as $n \rightarrow \infty$, and since all conjugates of $f(\alpha)$ are distinct, then there exists a positive integer $N \geq N_0$ for which

$$\sigma_{n+1} = \sigma_n \quad \text{if } n \geq N.$$

Hence, $p_n(\alpha) = 0$ for all $n \geq N$, and the theorem is proved.

Theorem 4. Let $f(z) = \sum_{h=0}^{\infty} a_h z^h$ be an Eisensteinian series convergent in $|z| < R$, for some fixed positive number R . Let b be a rational number such that $0 < |b| < R$. If f satisfies the Mahler's gap condition as stated in Theorem 3, then $f(b)$ is either a rational or a transcendental number.

Proof. Suppose, to the contrary, that $f(b)$ is an algebraic irrational number, then by Theorem 3, there exist a positive integer $N = N(b)$ and an increasing sequence of positive integers (n_j) such that for all j , we have $S_{n_j} = S_{r_N}$, where S_n is as in Theorem 1, r_n as in Theorem 3. Consequently, the greatest prime factor p_n of S_n , as $n \rightarrow \infty$, either does not exist, or if it does, it is never infinite. This contradicts Theorem 1(2) and we are done.

DISCUSSION

We list here some open problems.

Problem 1. We know that a power series $\sum_{n=0}^{\infty} a_n z^n$ is rational if and only if the power

series $\sum_{n=0}^{\infty} a_n z^n / n!$ satisfies a linear differential equation with constant coefficients.¹⁴

Furthermore, it is not hard to verify that if a power series $\sum_{n=0}^{\infty} a_n z^n$ represents an

algebraic power series, then the power series $\sum_{n=0}^{\infty} a_n z^n / n!$ satisfies a linear differential

equation with polynomial coefficients. This follows from an observation that if the former series is algebraic, then the sequence (a_n) satisfies a linear difference equation with polynomial coefficients for all sufficiently large n , and so the sequence $(a_n/n!)$ also

2. Güting, R. Approximation of Algebraic Numbers by Algebraic Number. *Michigan Math. J.*, 1961, **8**, 149-156.
3. Heine, E. Über die Entwicklung von Wurzeln Algebraischer Gleichungen in Potenzreihen. *J. reine angew. Math.*, 1854, **48**, 267-275.
4. Hurwitz, A. Sur le Développement des Fonctions Satisfaisant a une Equation Différentielle Algébrique. *Ann. de l' Ecole Norm. Sup.*, 1889, **6**, 327-332.
5. Kakeya, S. On a Power Series with Rational Coefficients Satisfying an Algebraic Differential Equation. *Science Reports Tôhoku Imp. Univ.*, 1915, **4**, 7-20.
6. Kongsakorn, K. and Laohakosol, V. A Generalization of Eisenstein's Theorem. *Bull. Inst. Math. Acad. Sinica*, 1986, **14**, 149-162.
7. Königsberger, L. Über den Eisensteinschen Satz von dem Charakter der Koeffizienten der Reihenentwicklungen Algebraischer Funktionen. *J. reine angew. Math.*, 1905, **130**, 259-269.
8. Landau, E. Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gausschen Differentialgleichung. *J. reine angew. Math.*, 1904, **127**, 92-102.
9. Laohakosol, V. An Arithmetic Property of the Taylor Coefficients of Analytic Functions with an Application to Transcendental Numbers. *Proc. Am. Math. Soc.*, 1985, **93**, 212-214.
10. Mahler, K. Arithmetic Properties of Lacunary Power Series with Integral Coefficients. *J. Austral. Math. Soc.*, 1965, **5**, 56-64.
11. Mahler, K. Lectures on Transcendental Numbers, Lecture Notes in Math. No. 546. Springer-Verlag, Berlin-Heidelberg-New York, 1976.
12. Pincherle, S. Sur la Nature Arithmétique des Coefficients des Series Intégrales des Equations Différentielles linéaires. *J. reine angew. Math.*, 1888, **103**, 84-86.
13. Pólya, G. Über das Anwachsen von ganzen Funktionen; die einer Differentialgleichung genügen. *Vierteljahrschr. Naturforsch. Gesellschaft Zurich*, 1916, **61**, 531-545.
14. Pólya G. and Szegő, G. Problems and Theorems in Analysis: Volume II. Springer-Verlage, New York-Heidelberg-Berlin, 1976.
15. Popken, J. Über Arithmetische Eigenschaften Analytischer Funktionen. N.V. Noord-Hollandsche Uitgeversmaatschappij, Amsterdam, 1935.
16. Popken, J. An Arithmetical Property of a Class of Dirichlet Series. *Indag. Math.*, 1945/46, **7**, 105-122.
17. Popken, J. Arithmetical Properties of the Taylor Coefficients of Algebraic Functions. *Proc. Kon. Ned. Akad. Wetensch.*, 1959, **62**, 202-210.
18. Stäckel, P. Arithmetische Eigenschaften Analytischer Funktionen. *Acta Math.*, 1902, **25**, 371-383.